CCPA

Who is it for?

✓ For-profit qualifying businesses must comply

✓ Protects residents of California (+their data)

Data collection rules:

✓ Make it easy to opt out of data collection

✓ Anonymized data counts as personal data

✓ Certain types of data require special handling

✓ Easy-to-read, detailed Privacy Policy required

✓ Confirm privacy request reciept within 10 days and respond within 45 days

Consumer rights:

✓ Right of access

✓ Right to deletion/ blocking/ restriction

✓ Right to data portability

✓ Right to opt out

✗ Right to object to automated decision making

✗ Right to rectification (not mentioned)

More compliance requirements

✗ DPO not required

✓ Document each privacy request and response

Fines

✓ Fines applied per violation, plus civil liability

Security and Liability

✗ CCPA does not explicitly require encryption. However, encryption can reduce a company's liability arising out of a data breach under both the CCPA and the GDPR. If a company suffers from a breach but the data was encrypted, some or all of the company's liability can be reduced.

Our compliance software:

DataMapper finds and tracks your company's sensitive data across employees, cloud storage, systems and apps. Sensitive data is sorted by risk level, and you can see where it is and who has access to it, making it easy to evaluate and monitor your data storage practices.

Request Manager automates the data privacy request process by receiving and verifying requests, quick data collection, encryption for data you send, notifications and documentation of every step in the data request process.

ShareSimple lets you share sensitive data with anyone in the world safely, with no certificates required, from the email you already use. It also gets and logs consent before accepting any personal data you request from others.

bysafeonline.com

GDPR

Who is it for?

✓ All public/private organizations must comply

✓ Protects anyone in the EU (+their data)

Data collection rules:

✓ Get explicit consent before processing data

✓ Excludes anonymized/pseudonymized data

✓ Sensitive data requires special handling

✓ Easy-to-read, detailed Privacy Policy required

✓ Respond to privacy requests within 30 days

Data subject rights:

✓ Right of access

✓ Right to deletion/ blocking/ restriction

✓ Right to data portability

✓ Right to object

✓ Right to object to automated decision making

✓ Right to rectification

More compliance requirements

✓ DPO required

✓ Record your data processing activities

Fines

✓ Max fine €20 million/4 percent annual revenue

Security and Liability

✓ Technical and organizational security measures may include: Encryption and pseudonymization of data, ensuring integrity, confidentiality, and availability of processing system; restoring the availability and access to personal data promptly; assessing and evaluating the effectiveness of technical and organizational measures.

Our compliance software:

DataMapper finds and tracks your company's sensitive data across employees, cloud storage, systems and apps. Sensitive data is sorted by risk level, and you can see where it is and who has access to it, making it easy to evaluate and monitor your data storage practices.

Request Manager automates the data privacy request process by receiving and verifying requests, quick data collection, encryption for data you send, notifications and documentation of every step in the data request process.

ShareSimple lets you share sensitive data with anyone in the world safely, with no certificates required, from the email you already use. It also gets and logs consent before accepting any personal data you request from others.

bysafeonline.com